

NETWORK IDENTIFICATION

After reading this chapter and completing the exercises, you will be able to:

- ◆ Explain the naming protocols used in Windows 2000 Server
- ◆ Configure the Microsoft Domain Name Service for Windows 2000 Server
- ◆ Install and manage the Microsoft Windows Internet Name Service for Windows 2000 Server
- ◆ Assign TCP/IP addressing information to clients dynamically using the Microsoft Dynamic Host Configuration Protocol service for Windows 2000 Server
- ◆ Create DHCP scopes, superscopes, and multicast scopes
- ◆ Understand the basic concepts underlying TCP/IP subnets and domains

This chapter discusses the components that allow Windows 2000 Server to resolve names and TCP/IP addresses. Three main services in Windows 2000 Server take care of this task: **Domain Naming Service (DNS)**, **Windows Internet Naming Service (WINS)**, and **Dynamic Host Configuration Protocol (DHCP)**. DNS resolves TCP/IP addresses to Internet names, WINS resolves TCP/IP addresses to NetBIOS names, and DHCP assigns TCP/IP addresses to clients dynamically.

USER IDENTIFICATION VERSUS COMPUTER IDENTIFICATION

It is important to understand the differences in how systems recognize users and other computers. In the following sections, you will see why it is necessary to differentiate between them and how Windows 2000 networks handle the different names.

Users

A user is simply a name and password combination that is assigned to a specific person. After a person receives a user name, he or she is considered a user and you can assign permissions and attributes to that user. For example, you can assign the user the rights to print to specific printers or to access certain resources.

NetBIOS Names

NetBIOS names are names that are assigned to computers in a Windows NT or 95/98 network. For backward compatibility, Windows 2000 must also use NetBIOS names. A NetBIOS name can have a maximum length of 15 characters, but may have a hidden sixteenth character, which is used to identify the service that will be accessed on the server.

MACHINE IDENTIFICATION AND NAME RESOLUTION

Computers communicate with one another using their hardware and protocol addresses. People find it difficult to remember long strings of numbers (and letters in the case of hardware addresses). Consequently, computers usually have two names for things: the names the computers understand, and the names humans understand. As a result, a method is needed for converting between these names and their addresses. This process is known as **name resolution**.

Domain Name Service

Windows 2000 Server relies heavily on Internet technologies and, therefore, on Internet naming conventions, known as domains. It is important to differentiate between a Windows 2000 domain and an Internet domain. The distinction is covered in detail in the “Domains” section later in this chapter. For now, simply remember that we are dealing with Internet domains.

Like most Windows 2000 Server services, DNS requires that the server be configured with a static IP address. By default, Windows 2000 Server configures itself as a client. You must assign it a unique, static IP address. You also need to give it a host name and a domain name.



When Active Directory is installed on a Windows 2000 Server computer, you are prompted either to have the Active Directory installation wizard configure your DNS or to manually configure DNS. Hands-on Project 9-1 details how to install DNS manually.

Zones

Microsoft DNS divides domain namespaces into **zones**. A zone is simply a logical group of addresses. For example, Microsoft.com is a zone, as is Seattle.Microsoft.com. All zone information is stored in a **zone database file**, which is a simple text file (assuming that you configure the zone as a standard zone, as described next) that is used by DNS to resolve TCP/IP names and addresses.

Windows 2000 Server DNS allows you to configure one of three zone types. These zone types, as shown in Figure 9-1, are:

- **Active Directory-integrated zone.** This zone type integrates all host and TCP/IP address information for this zone into the Active Directory. This option gives you the security and flexibility of Active Directory, while allowing Active Directory replication to update all zone information between servers. Creating an Active Directory-integrated zone is covered in Hands-on Project 9-4.
- **Standard primary zone.** This zone type, also known as a **master zone**, stores the original information for the zone. It is referred to as the authority for the zone or the domain, because it is in charge of all changes to the zone. Each zone can have a single standard primary zone. All zone information is stored in a text file, which is located in the %systemroot%\system32\dns directory. Creating a standard primary zone is covered in Hands-on Project 9-2.
- **Standard secondary zone.** This zone type stores a copy, or replica, of the standard primary zone information. The information is stored in a read-only format and is used for fault tolerance if the primary zone is not available. Multiple standard secondary zones can be configured on a network. As with standard primary zones, all secondary zone information is stored in a text file, which is located in the %systemroot%\system32\dns directory. Creating a standard secondary zone is covered in Hands-on Project 9-3.



Primary and secondary zones do not need to reside on the same physical network. Instead, they can exist in different companies, cities, states, or countries.

As noted earlier, zone information is stored in a zone database file. This file contains the name resolution information for the zone, known as **resources**. Several resource types exist in the Windows 2000 Server implementation of DNS. Some of the most common ones are listed in Table 9-1. By default, the zone database file carries a .dns extension.

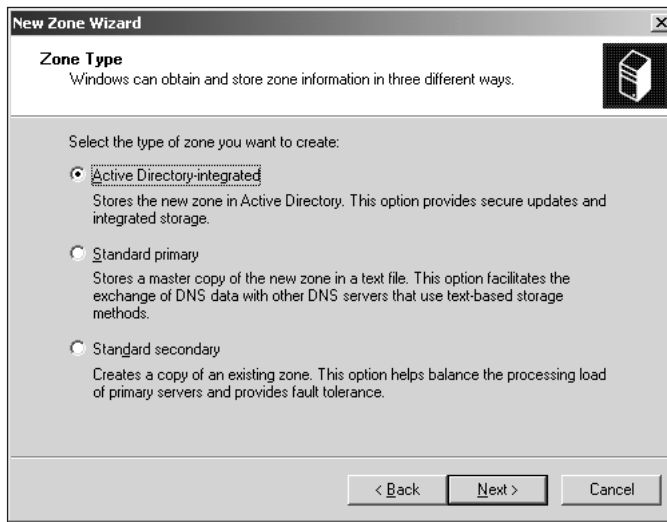


Figure 9-1 Windows 2000 Server zone types

Table 9-1 Domain Name Service resource types

Resource Record Type	Abbreviation	Definition
Start of Authority	SOA	Affects how a zone transfer takes place.
Name Server	NS	Defines one or more name servers as servers that will resolve names and IP addresses for this domain.
Mail Exchanger	MX	Identifies the server on the domain that is to receive e-mail messages for the domain.
Address	A	Used to resolve a TCP/IP host name to a TCP/IP address. Also known as a forward lookup.
Pointer	PTR	Used to resolve a TCP/IP address to a TCP/IP host name. Also known as a reverse lookup.
Canonical Name	CNAME	Defines aliases (if any) assigned to a TCP/IP host. A single host can have an unlimited number of aliases (or "nicknames").
Service Location	SRV	Defines a remote server that hosts a specific service, such as Kerberos, FTP, LDAP, or HTTP.
Windows Internet Name Service	WINS	Defines a server used to resolve Windows NT NetBIOS names (covered later in this chapter).

The configuration of most of these resource records is self-explanatory (and Windows 2000 Server automates most of the configuration).

SOA

One resource record that should be explored in some detail is the **Start of Authority (SOA)**, which affects how a zone transfer takes place (covered later in this chapter). Five numerical values make up the SOA. These values and their functions are as follows:

- *Serial Number*. A number used to track changes in the zone database file. Every time a change is made to the database, this variable is incremented by 1. It ensures that all changes are transferred to secondary zones. It is common to use a serial number in the form, YYYYMMDD## (for example, 1999090901 for the first change on September 9, 1999). This number not only tracks the changes, but also allows you to monitor when changes last took place.
- *Refresh Interval*. The amount of time (in seconds) that a secondary server waits before refreshing its zone database (assuming that changes exist) with the primary server.
- *Retry Interval*. The amount of time (in seconds) that the secondary server waits if it fails to contact the primary server for a zone database refresh. This value is used only if the primary database cannot be contacted.
- *Expire Interval*. The amount of time (in seconds) that the secondary server maintains a zone database, assuming that it cannot contact the primary database for updates. After this interval is reached, the secondary server stops resolving names and addresses.
- *Minimum Time-to-Live (TTL)*. The amount of time (in seconds) that the query response remains valid. After the TTL reaches zero, the query response is no longer valid and the DNS server must be requeried. This method ensures that any changes to the databases will eventually reach all systems on the network or Internet.

Zones are most commonly used in one of two ways: as **forward lookup zones** or as **reverse lookup zones**. These two ways are basically mirror images of one another. One is used to find the other. Creating a reverse lookup zone is detailed in Hands-on Project 9-5.

A forward lookup zone can contain any of the resource types (except a PTR record). The most common type of record that is stored in a forward lookup zone is the **Address (A) resource record**. Given a fully qualified domain name (FQDN), such as www.sprockets.com, this zone file is used to resolve it to the FQDN's TCP/IP address. In other words, when the DNS server is queried for the FQDN, it returns the IP address to the client. An example of a forward lookup file follows:

```
; Database file sales.sprockets.com.dns for sales.
sprockets.com zone.
;   Zone version: 1
;
```

```

@           IN  SOA  dns1.sprockets.com.  administrator.
sprockets.com. (
                    1           ; serial number
                    900          ; refresh
                    600          ; retry
                    86400         ; expire
                    3600         ) ; minimum TTL

;
;   Zone NS records
;

@           NS   dns1.sprockets.com.
@           NS   dns.provider.net.

;
;   Zone records
;

gateway     IN   A    10.0.0.1
www         IN   A    10.0.0.2
ftp         IN   A    10.0.0.3
mail        IN   A    10.0.0.4
dns1        IN   A    10.0.0.5
pop         IN   CNAME mail.sprockets.com.
smtp        IN   CNAME mail.sprockets.com.

mail        IN   MX   10    mail.sprockets.com.

```

Reverse lookup zones usually contain only PTR records. These records are used when a client system queries the server for the FQDN of a system given its TCP/IP address. Many Internet sites today will not grant access to information (such as downloads) unless their system can perform a reverse lookup on the TCP/IP address. An example of a reverse lookup zone file follows:

```

;   Database file 0.0.10.in-addr.arpa.dns for 0.0.10.in-
;   addr.arpa zone.
;   Zone version: 1
;

@           IN  SOA  dns1.sprockets.com.  administrator.
sprockets.com. (
                    1           ; serial number
                    900          ; refresh
                    600          ; retry
                    86400         ; expire
                    3600         ) ; minimum TTL

;
;   Zone NS records
;

```

```

@                NS      dns1.sprockets.com.

;
;  Zone records
;

1                IN      PTR    gateway.sprockets.com.
2                IN      PTR    www.sprockets.com.
3                IN      PTR    ftp.sprockets.com.
4                IN      PTR    mail.sprockets.com.
5                IN      PTR    dns1.sprockets.com.

```

Zone Transfers

The process of transferring information between standard primary and standard secondary servers is known as **zone transfer**. A zone transfer occurs when one of three events takes place:

- The primary server notifies a secondary server(s) of any changes within its databases.
- A secondary server contacts the primary server for any changes during the DNS service start-up.
- The refresh interval ends (as listed in the SOA record).

Two types of zone transfers exist: **Full Zone Transfer (AXFR)** and **Incremental Zone Transfer (IXFR)**.

The AXFR technique is the most commonly used method of transferring information between zones. It is compatible with most current implementations of DNS (independent of operating system). After the refresh interval on the secondary name server expires, this server contacts the primary name server and requests the SOA record. It then compares the serial number of this SOA record with the one stored in its configuration of the zone. If the serial numbers are the same, no zone transfer takes place. If the serial numbers are different, the secondary server assumes that its database information is outdated, and it copies the entire zone database from the primary server to its own database.

IXFR is a new method of updating zone information found in Windows 2000 Server. As with AXFR, the secondary server requests the SOA record from the primary server after its refresh interval expires. If the serial numbers match, no zone transfer takes place. If the serial numbers do not match, however, the secondary server requests only the changed records. This zone transfer method greatly increases performance between the primary and secondary servers, while minimizing network traffic, especially in environments with a large number of hosts in their DNS databases.

Windows Internet Name Service

Before Windows 2000 Server became available, Windows 95/98/NT relied on the NetBIOS protocol. Windows 2000 Server will not run in a true NetBIOS environment. If only one non-Windows 2000 system is installed on your network, however, NetBIOS becomes a necessity. For this reason, Windows 2000 Server ships with WINS. WINS is to NetBIOS names as DNS is to

TCP/IP names. That is, it simply allows for a dynamic conversion between a NetBIOS name and its TCP/IP address. WINS installation is detailed in Hands-on Project 9-6.

Four forms of communication between the WINS client and the WINS server are possible:

- Name registration
- Name query
- Name release
- Name renewal

You can configure primary and secondary WINS servers for each client. The client will attempt to contact the primary WINS server three times. If the primary WINS server does not respond, the client contacts the secondary WINS server.



If the primary server cannot resolve an address query, the secondary server is not contacted. A secondary server is contacted only if the primary server is not available. Each of these tasks is covered in detail in the following sections.

Name Registration

Every client that is configured to communicate with the WINS server contacts the server every time it boots and is initialized. The client sends a name registration request message to the WINS server that contains the following information:

- Its TCP/IP address (source)
- The WINS server's address (destination)
- The name to register (its NetBIOS name)

After the WINS server receives the registration request, it checks its database to see whether the name has already been registered. If it has, the WINS server attempts to contact the system that originally registered the name (it makes this attempt three times). If the original system responds, the requesting system is sent a negative name registration and the client is notified of the name conflict.

If the original registrant cannot be contacted, the WINS server drops it from its database and creates a new entry for the requesting system consisting of its NetBIOS name and TCP/IP address. The server responds to the client with the following information:

- Its TCP/IP address (source)
- The client's destination address
- The name that was registered
- A TTL that is assigned to the name

If the client cannot contact the primary WINS server, it attempts to contact the secondary WINS server. If that server does not respond, the client attempts to broadcast a registration

request. It then becomes the responsibility of the individual clients to inform the requesting client of any name conflicts on the network.

Name Query

After the client has registered its name and address with the WINS server, it can query the server for the addresses of any computers that it may need to contact. It does not, however, contact the WINS server first. Instead, it follows these steps:

1. The client system checks its NetBIOS cache to see whether it still has a record of the remote system's address.
2. If the cache does not contain the desired information, the client queries the primary WINS server for the remote system's address.
3. If neither WINS server can be contacted or the queried name does not exist in the WINS database, the client broadcasts its request. The system that has the broadcasted name will respond with its TCP/IP address.



You can view the current NetBIOS cache by issuing the *nbtstat -c* command from an MS-DOS prompt. To review *nbtstat* parameters, type *nbtstat ?* at the command prompt (see Figure 9-2).

9

```

C:\>nbtstat ?

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]

-a <adapter status> Lists the remote machine's name table given its name
-A <Adapter status> Lists the remote machine's name table given its
                    IP address.
-c <cache>          Lists NBT's cache of remote [machine] names and their
addresses
-n <names>          Lists local NetBIOS names.
-r <resolved>       Lists names resolved by broadcast and via WINS
-R <Reload>         Purges and reloads the remote cache name table
-S <Sessions>       Lists sessions table with the destination IP addresses
-s <Sessions>       Lists sessions table converting destination IP
                    addresses to computer NETBIOS names.
-RR <ReleaseRefresh> Sends Name Release packets to WINS and then, starts Re
esh

RemoteName Remote host machine name.
IP address Dotted decimal representation of the IP address.
interval Redisplays selected statistics, pausing interval seconds
          between each display. Press Ctrl+C to stop redisplaying
          statistics.

C:\>_
  
```

Figure 9-2 nbtstat parameters

Name Release

When a system no longer requires that its NetBIOS name be registered in the WINS server database, it sends a request to have the entry removed. This operation usually occurs when

either the system name changes or the system is shut down (or rebooted). The client sends the following information with its name release request:

- Its TCP/IP address (source)
- The WINS server's TCP/IP address (destination)
- The name to release

After the WINS server receives the name release request, it queries its database for the information. If it does not find the name of the requesting computer, it sends a negative name release message back to the client. If the WINS server finds the client's name in its database, it responds with the following information:

- The WINS server's TCP/IP address
- The client's TCP/IP address
- The name that was originally leased
- A TTL set to zero

After the client receives a name with the TTL set to zero, it releases its name and continues with either its shutdown process or its renaming process. The WINS server is not contacted again until the system is restarted or the client attempts to register the new name.

Name Renewal

WINS clients are configured to renew their registrations at set intervals. A WINS client attempts to contact its WINS server using the following criteria:

1. The client attempts to contact the primary WINS server at one-eighth of the TTL.
2. If no response is returned, the client attempts to renew its name registration every two minutes until one-half of the TTL has expired.
3. If the primary WINS server does not respond after one-half of the TTL has expired, the client sends a name registration renewal request to the secondary WINS server. At this point, the client treats the request as the first request.
4. The client sends a request every one-eighth of the TTL until one-half of the TTL has expired.
5. The client attempts to contact the primary WINS server again.
6. After a client has renewed its registration the first time, it attempts to contact the WINS server (to renew its registration) at one-half of the TTL.

Dynamic Host Configuration Protocol

DHCP is a protocol in the TCP/IP suite that is designed to ease a network administrator's job. The Windows 2000 DHCP service automatically assigns TCP/IP configuration information to your workstations. This scheme ensures that most TCP/IP addressing network

problems are eliminated. It is accomplished by having the server running the DHCP service lease addresses and other TCP/IP information to client systems. Installation of the DHCP service is detailed in Hands-on Project 9-7.

By default, Windows 2000 systems are configured as DHCP clients. When the client starts, it requests a TCP/IP address from a DHCP server. The **DHCP lease** consists of three mandatory values and several optional ones. At the least, the server must assign clients their own unique TCP/IP address, as well as a subnet mask and a TTL for the lease. Optional parameters include the following:

- A default gateway address
- The domain name
- The TCP/IP address of one or more DNS servers
- The TCP/IP address of one or more WINS servers
- The TCP/IP address of one or more Simple Mail Transfer Protocol (SMTP) servers

The DHCP server responds to any DHCP client request by offering it a TCP/IP address. This process is known as DHCP lease generation.

9

The DHCP Lease

The DHCP lease is a four-phase process. These four phases are as follows:

- DHCPDISCOVER
- DHCPOFFER
- DHCPREQUEST
- DHCPACK

DHCPDISCOVER As you can imagine, when a DHCP client is first initialized, it knows nothing about the network. It does not know its TCP/IP address, subnet mask, or even the address of the DHCP server. To discover this information, it “yells”—stated in more technical terms, it sends a broadcast, which is known as a DHCPDISCOVER message.

Because the client does not have its own dedicated TCP/IP address, it sends its IP address as 0.0.0.0, transmitting this message to the TCP/IP address 255.255.255.255 (producing a complete broadcast). Every computer on the local network hears this message, but only systems that are configured as DHCP servers respond. The DHCP server (or servers) may receive a large number of requests simultaneously; as a consequence, the client includes its hardware address (or MAC address) and its computer name.

DHCPOFFER All DHCP servers “hear” the broadcast and the ones with TCP/IP addresses available to lease to the client respond. Because the client still does not have a unique

TCP/IP address configured, the DHCP server broadcasts the information. Broadcasting the DHCPOFFER message performs two important tasks:

- It notifies the DHCP client that a TCP/IP address is being offered to it.
- It notifies any other DHCP servers on the network that an offer has been made. It is important to remember that all DHCP servers with available TCP/IP address leases will offer one. The DHCPOFFER message just lets all of the servers know that other options exist for the client.

After the DHCP server offers a TCP/IP address to the client, it reserves that address so that it will not be offered to another client. The DHCP offer includes the following information:

- The client's hardware address (it is the only way to distinguish between different DHCP clients requesting TCP/IP addresses)
- The offered TCP/IP address
- The offered subnet mask
- The TCP/IP address of the DHCP server making the offer
- The length of the DHCP lease

DHCPREQUEST The DHCP client is not picky about which DHCP lease it accepts. It simply accepts the first one that it receives. After it has received the offer, it broadcasts a DHCPREQUEST message. Although the DHCP client has the required TCP/IP addressing information (although limited), it nevertheless broadcasts the DHCPREQUEST message. This message notifies any and all DHCP servers that made an offer that an offer has been accepted. After a DHCP server receives a DHCPREQUEST that is directed at a DHCP server other than itself, it retracts its TCP/IP offer and frees that address for another client. For this process to take place successfully, the client must include the TCP/IP address of the DHCP server from which it is accepting an offer.

DHCPACK The DHCP server that made the original offer sends a final message to the DHCP client in which it acknowledges the lease. The client is now notified (via a broadcast message) of the valid lease, and any other configuration information, such as **default gateway** or DNS servers, is sent to the client.

The DHCP client initializes the TCP/IP protocol stack and binds the protocol to any suitable network cards. At this point, the client can communicate with the network, because it now has a unique TCP/IP address on the network.



Because the client does not have its own unique TCP/IP address until all four of the previously mentioned messages are transferred, all communications between the client and the DHCP server are sent as broadcast messages.

The DHCP Lease Renewal

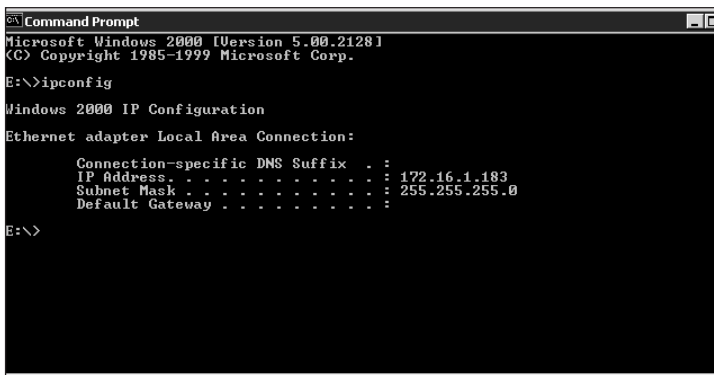
At some point, the DHCP lease expires. A lease can be renewed in two ways: by using the automatic lease renewal method, or by using the manual lease renewal method. Automatic

lease renewal occurs based on some specific rules, which are covered in the following section. Manual renewal allows an administrator or user to renew the lease at any time. The manual lease renewal is also employed when changing from one DHCP server to another.

Automatic DHCP Renewal As with WINS, in DHCP the client renegotiates its lease with the DHCP server at set intervals. By default, the DHCP client attempts to renew the lease at 50 percent of the lease. For example, if the lease is set to 72 hours (3 days), the client attempts to renew the lease when 36 hours have passed (1.5 days). To accomplish this goal, it sends a directed DHCPREQUEST message (that is, it does not broadcast the message but it uses the TCP/IP address of the DHCP server). If the DHCP server is online, it responds to the message with a DHCPACK message. This message contains the length of the lease and any configuration information that needs to be updated. The client then updates its configuration to match the new information (if any) received from the server.

If the DHCP server that assigned the address to the client is not available, the client maintains its current TCP/IP configuration as originally assigned by the DHCP server. It attempts to contact the server again with a DHCPREQUEST message when seven-eighths (87.5 percent) of the lease has expired. Although the original DHCP server can respond with a DHCPACK message, any DHCP server can respond to the DHCPREQUEST message with a DHCPNACK. This response forces the client to drop its DHCP lease and attempt to lease a different one.

Manual DHCP Lease Renewal You may find a need to release the DHCP-assigned address from a client, such as during a DHCP reservation or when moving a system from one network to another. In such situations, you can manually release and/or renew the DHCP addresses. To accomplish this task, you need to run the IPCONFIG application from a command prompt (see Figure 9-3).



```

C:\> Command Prompt
Microsoft Windows 2000 [Version 5.00.21281]
(C) Copyright 1985-1999 Microsoft Corp.

E:\> ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    IP Address . . . . . : 172.16.1.183
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

E:\>
  
```

Figure 9-3 Output from ipconfig

To renew the DHCP-assigned address, you can issue the IPCONFIG /RENEW command. This command sends a DHCPREQUEST message to the DHCP server that originally assigned it the TCP/IP address. In most cases, it does not change the TCP/IP address, but

simply updates any configuration changes from the server. If you configured a reservation, that reserved TCP/IP address is assigned.

In some situations, you may want the client to receive a new TCP/IP address either from the same DHCP server that assigned the previous address or from a new DHCP server. In such cases, you issue the `IPCONFIG /RELEASE` command, which forces the DHCP client to drop its entire DHCP configuration. At this point, the client is no longer able to communicate on the network. You must issue the `IPCONFIG /RENEW` command to restart the entire lease request process.

DHCP and Active Directory

To allow for greater control over DHCP in Windows 2000 Server, you must authorize all DHCP servers in Active Directory. A DHCP service will start only if it has been authorized. If no authorization has been issued, the service will fail.

When a DHCP server attempts to start, it broadcasts a change status message to Active Directory. If any changes in the authorization are detected, the DHCP server responds accordingly. This scheme allows you to deauthorize a server without having to visit the actual system on which the DHCP service is running. You would simply remove the authorization, and the DHCP service would stop the next time it detects the change.

DHCP Scopes

After the DHCP service is installed and running (and authorized in Active Directory), you need to configure a **DHCP scope**. A scope is simply a logical boundary that is assigned to TCP/IP addresses. That is, the scope is the “pool” of addresses from which the server is allowed to pull to lease to clients. When configuring the scope, you need to supply the following information:

- The name for the scope
- A description for the scope (optional)
- An address range
- A subnet mask
- A list of excluded addresses (optional)
- The length of the lease

In the New Scope Wizard (shown in Figure 9-4), you have the chance of configuring some DHCP options that may be sent to all DHCP clients. As stated previously, these options include the default gateway, host name, and DNS server addresses. Creating a DHCP scope is detailed in Hands-on Project 9-8.

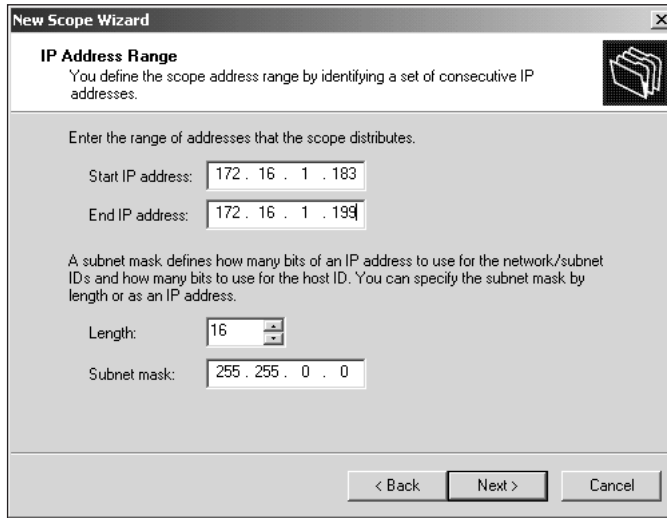


Figure 9-4 New Scope Wizard.

Windows 2000 Server also supports two other types of scopes: **superscopes** and **multicast scopes**. Superscopes are simply an administrative way to combine two or more scopes into a single administrative unit. They are most commonly used when a network grows beyond its original boundaries, requiring more than one scope to define it. Multicast scopes are designed for collaborative applications, such as streaming multimedia or conferencing. This type of scope allows you to send information to a single directed address and have the entire multicast group receive and process the information. Before multicast scopes existed, the only way to configure a multicast group was to manually assign addresses to the clients that were to participate. Hands-on Project 9-9 details how to create a superscope; the creation of a multicast scope is discussed in Hands-on Project 9-10.

NETWORK ORGANIZATION

Windows 2000 Server uses the TCP/IP networking and domain models as its network model. The next two sections define and examine subnets and gateways, as well as Internet (and Windows 2000) domains.

Subnets and Gateways

A **subnet** is a logical boundary on your network. A computer uses the subnet mask to determine whether a system it is trying to contact is local or remote. Anything that exists within the same network is “local.” Likewise, any systems outside the subnet are “remote.”

You can think of a subnet as being analogous to a city. Any mail sent within the city is local; therefore, it can be delivered directly to the recipient. When you need to send a package to a resident in the city, you simply put enough local postage on it and drop it off at the post office. The post office then delivers the package to its destination.

When the package is destined for a remote location (such as another city or state), the post office recognizes that fact and sends the package to that site. It then becomes the responsibility of the remote site to deliver the package. For that remote site, the package becomes local.

With TCP/IP networks, the data are sent to the default gateway. Simply put, a default gateway is a device (a multihomed computer or a router) that can communicate between two networks. Any information that is destined to a remote system is passed to the default gateway and eventually sent to its destination.

Domains

Computers use TCP/IP and MAC addresses to find and contact each other. People do not have the ability to remember the TCP/IP addresses of systems. For example, if you were asked to give Microsoft's Web site address, you would answer *www.microsoft.com*. If you were asked to give Microsoft's TCP/IP or MAC address, however, you would most likely need to look up that information. To simplify the naming conventions, domains were created.

Domains are analogous to the root system for a tree (see Figure 9-5). At the top of the tree, you find the root. The root is usually shown as a period (.), although this period is assumed and not usually written. Directly below the root are the top-level domains. They include .com, .org, .mil, .edu, and .net, as well as the various country codes (for example, .us, .ca, .uk).

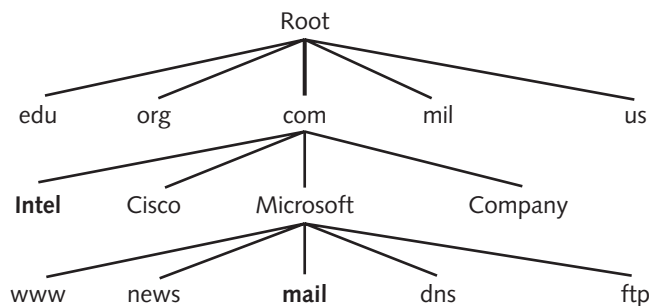


Figure 9-5 Domain structure

Below the top-level domains are the second-level domains, which are controlled by individual organizations. For example, Microsoft controls the Microsoft.com domain, and no other company can make changes to it. In contrast, no one really owns the top-level domains. They are controlled by InterNIC, the company that controls the registration of domain names.

CHAPTER SUMMARY

- Users are the people who access resources on the network. At a minimum, a user is granted a user name and a password. Users are also granted permissions to access and modify resources on the network.
- Three protocols exist in Windows 2000 to assist with name resolution and address assignment. DNS bridges the gap between TCP/IP addresses and Internet names, whereas WINS resolves TCP/IP addresses and NetBIOS names. DHCP is a protocol that is used to dynamically assign TCP/IP addresses and other network-related values—such as the default gateway, DNS server, or WINS server—to computers.
- A Windows 2000 network is made up of subnets. Subnets are simply logical boundaries that are set on networks. For networks to communicate with each other between subnets, a device (either a router or a default gateway) must be present that passes information between the networks.

KEY TERMS

Active Directory-integrated zone — A zone that allows for Active Directory security to control replication of the database information.

Address (A) resource record — An address resolution from a regular name to a TCP/IP address.

Canonical Name — An alias that can be assigned to a TCP/IP host.

default gateway — A device (a multihomed computer or a router) that can communicate between two different networks.

DHCP lease — An IP address, subnet mask, and optional parameters that are given to a DHCP client for a configured amount of time.

DHCP scope — A logical grouping of TCP/IP addresses that can be assigned to DHCP clients by the server.

Domain Name Service (DNS) — A dynamic method for resolving TCP/IP addresses to Internet names, and vice versa.

Dynamic Host Configuration Protocol (DHCP) — A protocol that allows for the automatic configuration of TCP/IP properties for clients.

forward lookup zone — The zone in charge of Internet name to TCP/IP address resolution.

Full Zone Transfer (AXFR) — A complete transfer of all zone information from the primary site to the secondary sites.

Incremental Zone Transfer (IXFR) — A partial transfer of modified zone information between the primary and secondary sites.

Mail Exchanger — A DNS record used to resolve which server in the domain takes charge of e-mail.

master zone — See *standard primary zone*.

- multicast scope** — A scope that is used to send collaborative information to a group of computers without the need to manually configure the clients.
- name resolution** — The method of converting between human-readable names and computer names and addresses.
- Name Server** — A DNS record that defines which server in the domain acts as the name server.
- Pointer** — A DNS record that resolves a TCP/IP address to its Internet name.
- resources** — Name resolution information for a zone.
- reverse lookup zone** — A zone that maintains the pointer records and resolves IP addresses to names.
- Service Location** — Allows you to configure services that are located on remote systems.
- standard primary zone** — The authority for the zone. It is in charge of all changes to the domains.
- standard secondary zone** — A read-only copy of the standard primary zone database. It is used for fault tolerance and load balancing.
- Start of Authority (SOA)** — A DNS record that defines the different timeout and TTL values for the domain.
- subnet** — A logical boundary on a network.
- superscope** — A process of combining two or more scopes to group them into a single administrative unit.
- Windows Internet Name Service (WINS)** — A service that resolves NetBIOS names (or computer names) to TCP/IP addresses.
- WINS** — A DNS record that defines the TCP/IP address of one or more WINS servers on the network.
- zone** — A logical group of addresses.
- zone database file** — A simple text file in a standard zone that is used by DNS to resolve TCP/IP names and addresses.
- zone transfer** — The process of transferring information between standard primary and standard secondary servers.

REVIEW QUESTIONS

1. Which of the following DHCP options is not a required value?
 - a. Default gateway
 - b. TCP/IP address
 - c. Subnet mask
 - d. Lease length
2. Windows 2000 Server domains and Internet domains are one and the same. True or False?

3. Which of the following is not a DHCP message?
 - a. DHCPDISCOVER
 - b. DHCPOFFER
 - c. DHCPREQUEST
 - d. DHCPACCEPT
4. A DHCP gateway must be authorized in the Active Directory before it can assign TCP/IP addresses. True or False?
5. A DHCP server can have a DHCP-assigned IP address. True or False?
6. After a scope is created, the subnet mask cannot be changed without deleting and recreating the scope. True or False?
7. Which of the following is not a zone type in Windows 2000 Server DNS?
 - a. Active Directory-integrated
 - b. Active Directory-authorized
 - c. Standard primary
 - d. Standard secondary
8. A Windows 2000 network does not require NetBEUI names to operate, so it does not require WINS. True or False?
9. A DHCP client will attempt to renew its lease at _____ percent of the lease time.
10. If a DHCP client cannot renew its lease at the amount of time specified in Question 9, it will attempt again at _____ percent of the lease time.
11. If the primary DNS server cannot resolve a name, the secondary server will attempt to resolve it. True or False?
12. Static mappings can be created with WINS. True or False?
13. What is a default gateway used for?
 - a. Communication with local networks
 - b. Communication with remote networks
 - c. Name resolution for TCP/IP names
 - d. Name resolution for NetBIOS names
14. Windows 2000 Server running DNS cannot act as a standard secondary zone to a Windows NT 4.0 Server. True or False?
15. DHCP is a Microsoft standard rather than an industry standard. True or False?

HANDS-ON PROJECTS



Project 9-1

To install the Domain Name Service:

1. Click **Start** and choose **Programs, Administrative Tools, Configure Your Server**.
2. Click the **Advanced** option in the left pane of the window and choose **Optional Components**.
3. Click **Start** in the right pane to start the Windows Component Wizard.
4. Highlight the **Networking Services** option and click **Details**.
5. Select the **Domain Name System (DNS)** option (as shown in Figure 9-6), and click **OK**.
6. Back in the Windows Component Wizard, click **Next** and complete the steps as prompted.

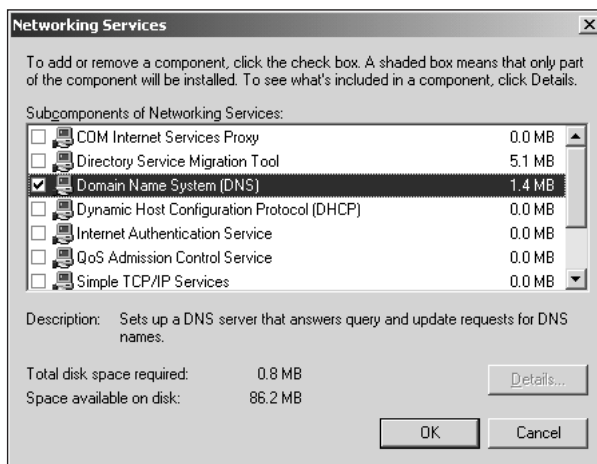


Figure 9-6 Setting up Domain Name Service



Project 9-2

To create a standard primary zone:

1. Click **Start** and choose **Programs, Administrative Tools, DNS**. (See Figure 9-7.)
2. Highlight the server in which you want to create the zone.
3. Click the **Action** menu and choose **New Zone**. The New Zone Wizard starts.
4. Click **Next**. Figure 9-8 is displayed and prompts you to choose the zone type.

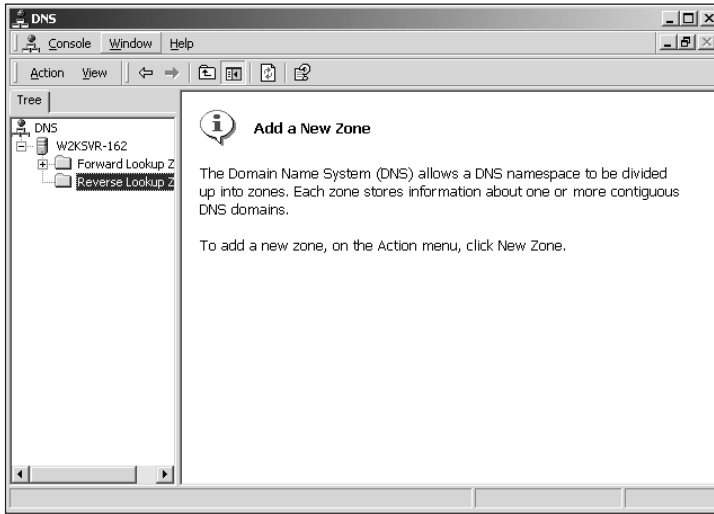


Figure 9-7 The DNS configuration tool

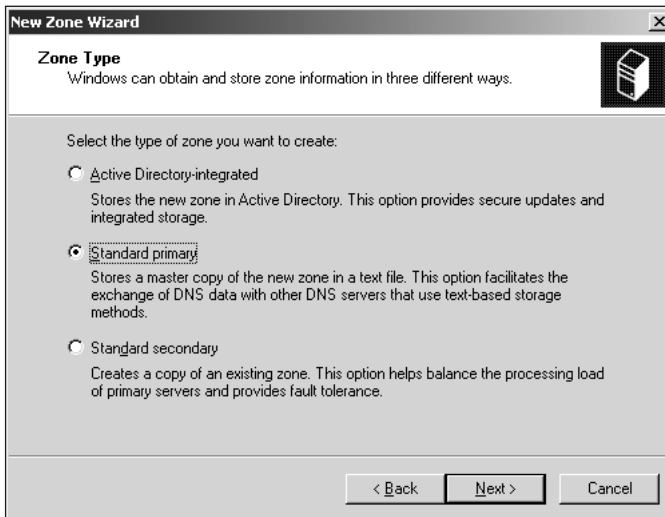


Figure 9-8 Configuring a standard primary zone

5. Select **Standard primary** and click **Next**.
6. In the **Name** field, enter a name to be assigned to this zone (it will usually be the domain name for which this DNS server is being configured). Click **Next**.
7. Choose either to create a new database file or to use an existing one. Notice that the filename is automatically created as the name assigned in Step 5 with the *.dns* extension added. Click **Next**.
8. Click **Finish** to complete the primary zone creation.



Project 9-3

To create a standard secondary zone:

1. Click **Start** and choose **Programs, Administrative Tools, DNS**.
2. Highlight the server in which you want to create the zone.
3. Click the **Action** menu and choose **New Zone**. The New Zone Wizard starts.
4. Click **Next**.
5. Select the **Standard secondary** option, and click **Next** (see Figure 9-9).

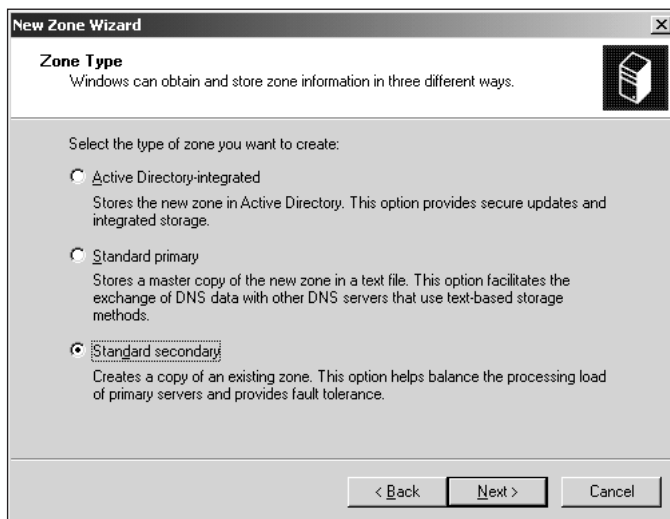


Figure 9-9 Configuring a standard secondary zone

6. In the **Name** field, enter a name to be assigned to this zone (it will usually be the domain name for which this DNS server is being configured). Click **Next**.
7. Enter the TCP/IP address of the primary zone server in the **IP Address** field, and click **Add**. Click **Next**.
8. Click **Finish** to complete the zone creation.



Project 9-4

To create a Active Directory-integrated zone:

1. Click **Start** and choose **Programs, Administrative Tools, DNS**.
2. Highlight the server in which you want to create the zone.
3. Click the **Action** menu and choose **New Zone**. The New Zone Wizard starts.
4. Click **Next**.
5. Ensure that the **Active Directory-integrated** option is selected, and click **Next** (see Figure 9-10).

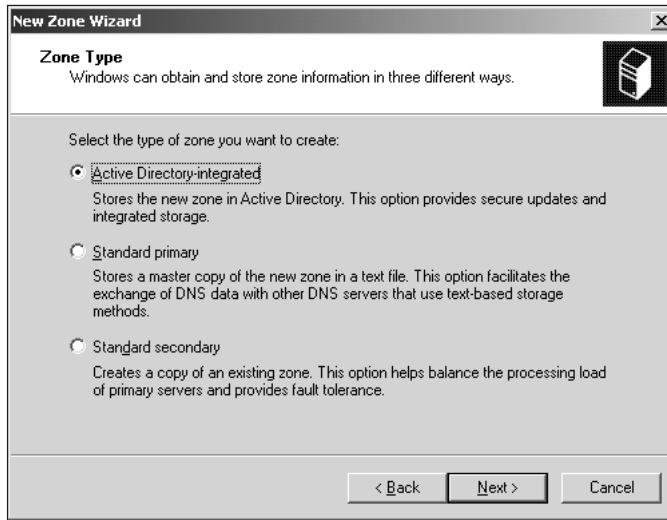


Figure 9-10 Configuring an Active Directory-integrated zone

6. In the **Name** field, enter a name to be assigned to this zone (it will usually be the domain name for which this DNS server is being configured). Click **Next**.
7. Click **Finish** to complete the zone creation.

9



Project 9-5

To create a reverse lookup zone:

1. Click **Start** and choose **Programs, Administrative Tools, DNS**.
2. Highlight the **Reverse Lookup Zones** option in the left pane. Click the **Action** menu and choose **New Zone**. The New Zone Wizard starts.
3. Click **Next**.
4. Choose the zone option that you would like to configure (**Active Directory-integrated**, **Standard primary**, or **Standard secondary**), and click **Next**.
5. Enter the **Network ID** (see Figure 9-11) or specify that you will manually create the reverse lookup zone. Click **Next**.
6. Choose either to create a new database file or to use an existing one (again, this file will have the **.dns** extension), and click **Next**.
7. Click **Finish**.

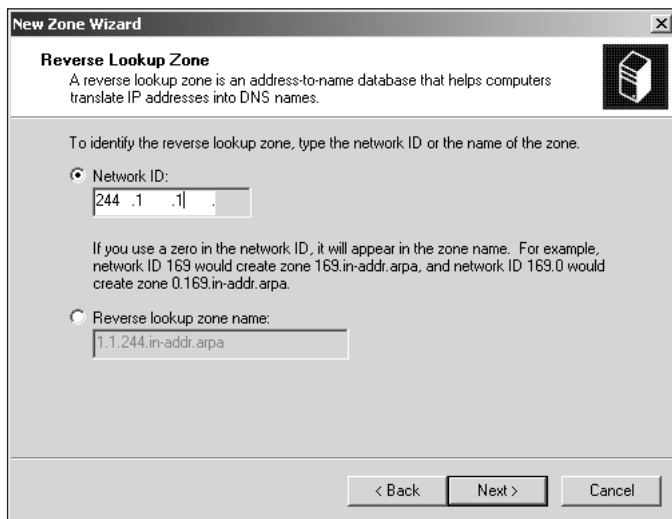


Figure 9-11 Configuring a reverse lookup zone



Project 9-6

To install the Windows Internet Name Service:

1. Click **Start** and choose **Programs, Administrative Tools, Configure Your Server**.
2. Click the **Advanced** option in the left pane of the window.
3. Choose the **Optional Components** selection from the left pane.
4. Click **Start** in the right pane to start the Windows Component Wizard.
5. Highlight the **Networking Services** option, and click the **Details** button.
6. Select the **Windows Internet Name Service (WINS)** option (as shown in Figure 9-12), and click **OK**.
7. In the Windows Components Wizard, click **Next**, then click **Finish**.



Project 9-7

To install the Dynamic Host Configuration Protocol service:

1. Click **Start** and choose **Programs, Administrative Tools, Configure Your Server**.
2. Click the **Advanced** option in the left pane of the window, and choose **Optional Components**.
3. Click **Start** in the right pane to start the Windows Component Wizard.
4. Highlight the **Networking Services** option, and click the **Details** button.
5. Select the **Dynamic Host Configuration Protocol (DHCP)** option (as shown in Figure 9-13), and click **OK**.
6. In the Windows Components Wizard, click **Next**, then click **Finish**.

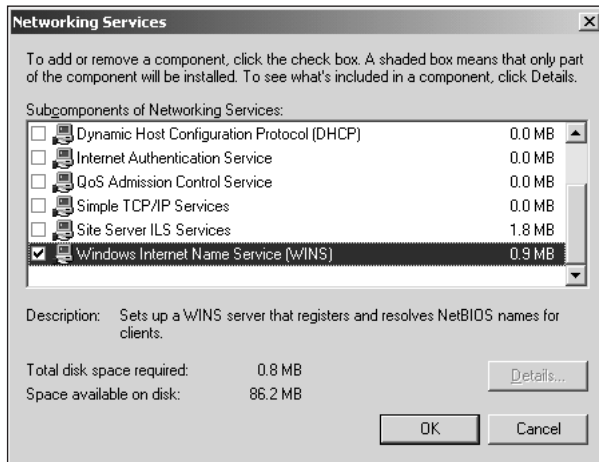


Figure 9-12 Setting up Windows Internet Naming Service

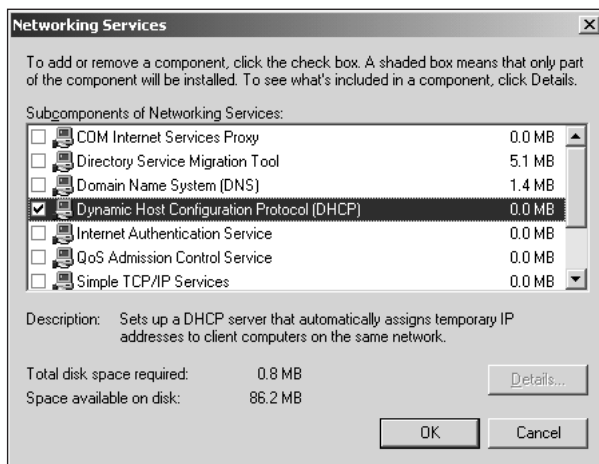


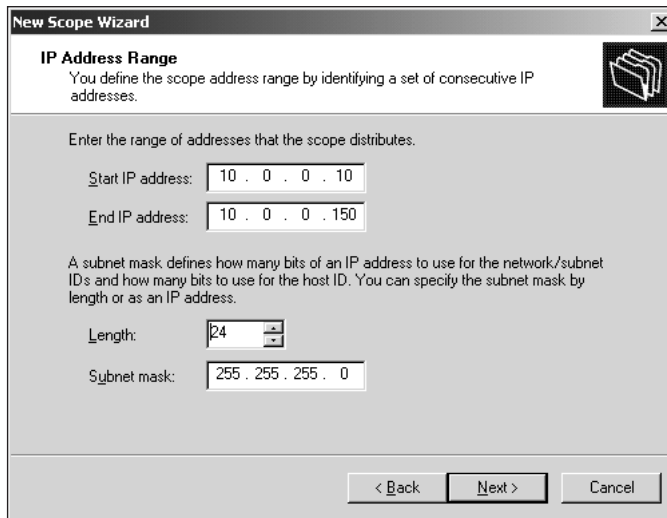
Figure 9-13 Setting up Dynamic Host Configuration Protocol



Project 9-8

To create a new DHCP scope:

1. Click **Start** and choose **Programs, Administrative Tools, DHCP**.
2. Select the server to configure, then, from the **Action** menu, choose the **New Scope** option. The New Scope Wizard starts.
3. Click **Next**.
4. Enter a name for the scope and an optional description, and click the **Next** button.
5. Enter the starting and ending TCP/IP addresses that will define this scope, as well as the subnet mask (see Figure 9-14). Click **Next**.



New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 10 . 0 . 0 . 10

End IP address: 10 . 0 . 0 . 150

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

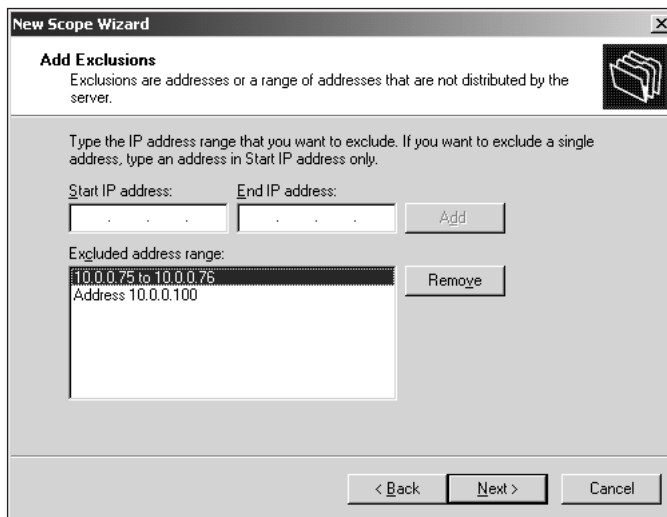
Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

Figure 9-14 Creating a DHCP scope

6. Enter any TCP/IP address exclusions (these include TCP/IP addresses of static systems such as servers), as shown in Figure 9-15. Click **Next**.



New Scope Wizard

Add Exclusions
Exclusions are addresses or a range of addresses that are not distributed by the server.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: . . . End IP address: . . . Add

Excluded address range:

- 10.0.0.75 to 10.0.0.76
- Address 10.0.0.100

Remove

< Back Next > Cancel

Figure 9-15 Excluding addresses within a DHCP scope



If you need to exclude a single TCP/IP address, simply enter the address for both the start and end address and click **Add**.

7. Enter the lease duration, and click **Next**.

8. You are now asked if you want to configure the optional settings now or later. If you choose to configure them now, you see three screens (Figures 9-16 through 9-18): Router (Default Gateway), Domain Name and DNS Servers, and WINS Servers, respectively.

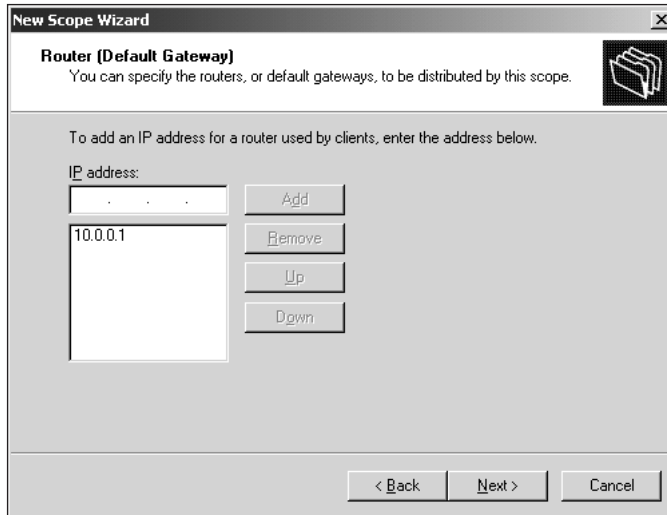


Figure 9-16 Configuring an optional default gateway with DHCP

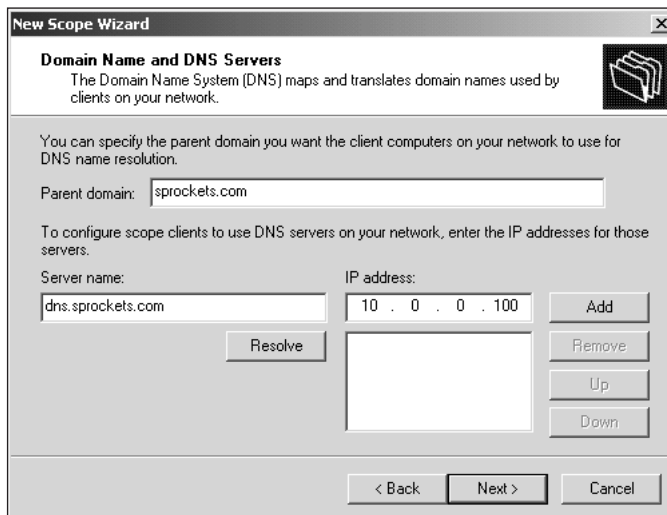


Figure 9-17 Configuring an optional DNS server with DHCP

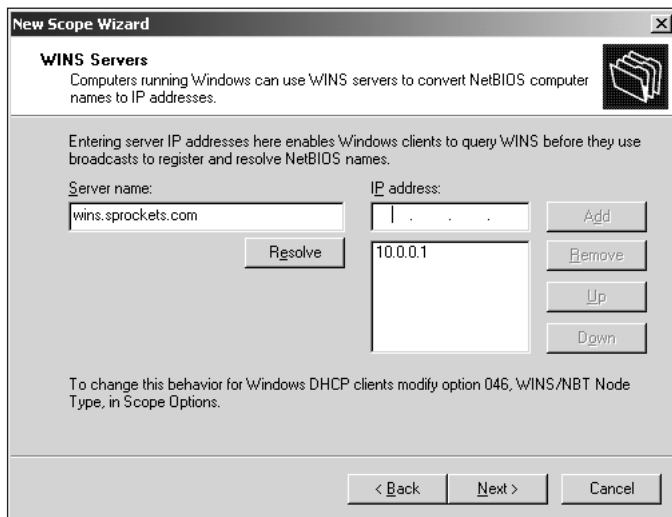


Figure 9-18 Configuring an optional WINS server with DHCP

9. Choose whether you will activate the scope. By activating the scope, you allow the DHCP server to start assigning IP addresses. Click **Next**.
10. Click **Finish**.



Project 9-9



To complete this project, please repeat Hands-on Project 9-8 and create a different scope so that two scopes are available to create the superscope.

To configure a superscope:

1. Click **Start** and choose **Programs, Administrative Tools, DHCP**.
2. From the **Action** menu, choose the **New Superscope** option. The New Superscope Wizard starts.
3. Click **Next**.
4. Enter a name for the superscope, and click **Next**.
5. Select two (or more) scopes to include in the superscope (see Figure 9-19), and click **Next**.

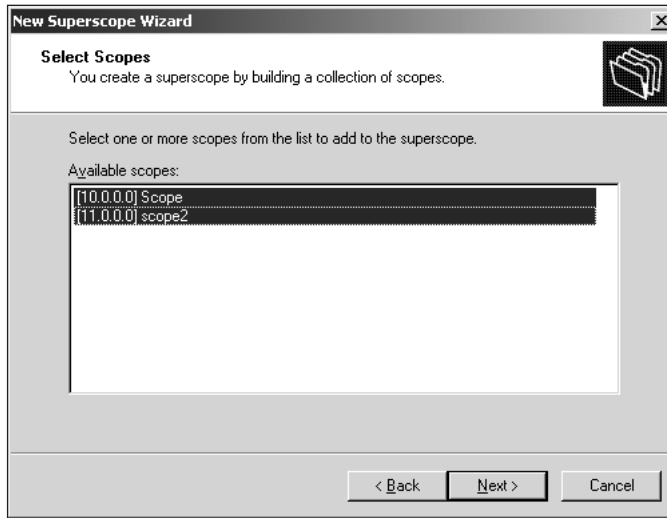


Figure 9-19 Setting up a superscope

6. Click **Finish**.

9



Project 9-10

To configure a multicast scope:

1. Click **Start** and choose **Programs, Administrative Tools, DHCP**.
2. From the **Action** menu, choose the **New Multicast Scope** option. The New Multicast Scope Wizard starts.
3. Click **Next**.
4. Enter a name and an optional description for the multicast scope, and click the **Next** button.
5. Enter a valid TCP/IP range (from 224.1.1.1 to 224.1.1.254), and click the **Next** button, as shown in Figure 9-20.
6. Add any address exclusions for this scope, and click **Next**.
7. Enter a value for the term of the lease (the default is 30 days), and click **Next**.
8. Choose whether to activate this multicast scope, and click **Next**.
9. Click **Finish**.

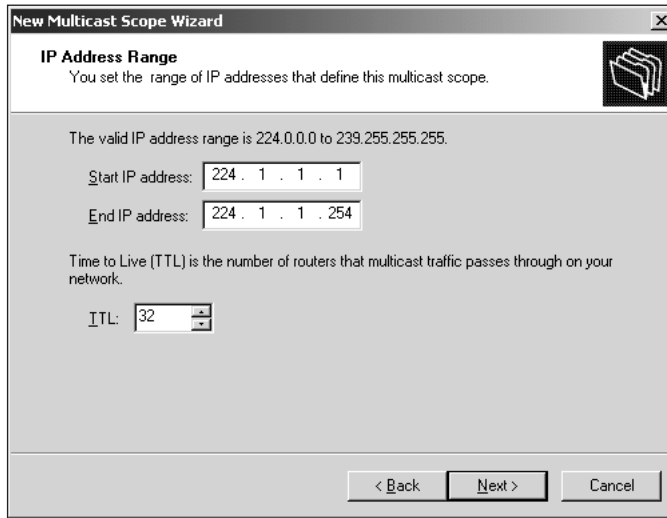


Figure 9-20 Setting up a multicast scope

CASE PROJECTS

1. You upgrade your network to a Windows 2000 network. You still have some Windows 95/98 systems on the network. Do you continue to require WINS to resolve names?
2. Your organization would like to connect to the Internet and control all of its Internet names and domains. Which Windows 2000 service would you need to implement?
3. As an administrator, you have been asked to implement a TCP/IP-based network. One task that you would like to avoid is the manual assignment of TCP/IP addresses to each of your network's workstations. Which Windows 2000 service would you install?
4. You currently have a Windows NT 4.0 network installed. You would like to upgrade your network to a Windows 2000 network with Active Directory. Do you have to upgrade the DNS servers to Windows 2000 dynamic DNS at the first step or the last? Why or why not?